PATENT ABSTRACTS OF JAPAN
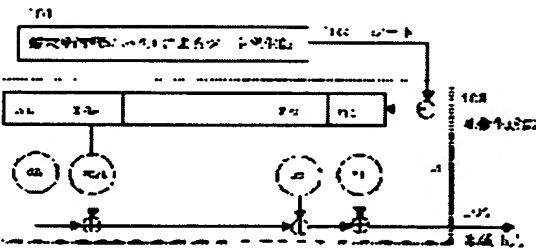
(11)Publication number :   2002-215030

(43)Date of publication of application : 31.07.2002

(51)Int.Cl.	G09C 1/00 G06F 7/58

(21)Application number : 2001-008638

(22)Date of filing :   17.01.2001

(71)Applicant : ADVANCED MOBILE TELECOMMUNICATIONS SECURITY TECHNOLOGY RESEARCH LAB CO LTD

(72)Inventor : KATO TAKEHIKO
MATSUZAKI NATSUME
ANZAI JUN
MATSUMOTO TSUTOMU

(54) RANDOM NUMBER GENERATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To generate secure random numbers without any external operation with a simple configuration in a mobile terminal.
SOLUTION: A part of information which is not repeatable to temporally irregularly change out of state information generated by a function means, which the mobile terminal has, like a terminal reception radio level is extracted and is taken as sample data. Sample data is inputted to a random number generation part 103 s a seed 102 to generate random numbers 104. Since the same random numbers are not generated from the next timing though the internal state at a certain point of time is copied, this method is safe. Random numbers of high quality can be generated without requiring addition of special parts and materials.

LEGAL STATUS

[Date of request for examination]	26.03.2001
[Date of sending the examiner's decision of rejection]	15.06.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	